

Message Text

SECRET

PAGE 01 GENEVA 12065 01 OF 02 132122Z
ACTION SS-25

INFO OCT-01 ISO-00 SSO-00 NSCE-00 DODE-00 CIAE-00
INRE-00 ACDE-00 ERDE-00 /026 W
-----031230 132128Z /73
O 132040Z DEC 77
FM USMISSION GENEVA
TO SECSTATE WASHDC IMMEDIATE 4023
INFO AMEMBASSY LONDON PRIORITY
AMEMBASSY MOSCOW PRIORITY

S E C R E T SECTION 01 OF 02 GENEVA 12065

EXDIS USCTB

PASS TO DOE

E.O.11652:XGDS-3
TAGS: PARM US UK UR
SUBJECT:CTB NEGOTIATIONS: INFORMAL TECHNICAL WORKING GROUP,
DECEMBER 13, 1977

CTB MESSAGE NO.85

1. SUMMARY: INFORMAL TECHNICAL WORKING GROUP HELD FIRST
MEETING ON DEC 13. TURNBULL READ AND PASSED TO SOVIETS
WORKING PAPER ON DATA AUTHENTICATION SYSTEM AND ANSWERED
QUESTIONS. UK ASKED SEVERAL SPECIFIC QUESTIONS; SOVIET
QUESTIONS WERE OF GENERAL AND EXPLORATORY NATURE. END
SUMMARY

2. INFORMAL TECHNICAL WORKING GROUP HELD FIRST MEETING
DEC 13 AT UK MISSION. PARTICIPATING WERE FAKLEY (UK
CHAIRMAN), WETHERELL, VEREY, AND BISHOP (INTERPRETER) FOR
UK, OSIN (USSR CHAIRMAN), BOCHAROV, NOVIKOV, BELOV,
PATRAKEYEV, KOSTYUCHENKO, AND POGODIN (INTERPRETER) FOR
SECRET

SECRET

PAGE 02 GENEVA 12065 01 OF 02 132122Z

USSR, AND TURNBULL (US CHAIRMAN), HECKROTTE, PHELPS, DUFF,
FROSCHE, AND SMITH (INTERPRETER) FOR US.

3. FAKLEY OPENED SESSION BY SAYING TASK OF GROUP SHOULD BE
TO PROVIDE BACKGROUND TECHNICAL INFORMATION TO ASSIST IN
FUTURE WORK AND TO ANSWER ANY TECHNICAL QUESTIONS THAT
REMAIN UNANSWERED FROM PLENARY MEETINGS. HE THEN TURNED

FLOOR TO TURNBULL, WHO READ, EXPLAINED, AND PASSED OVER WORKING PAPER ON DATA AUTHENTICATION SYSTEM FOR INTERNAL STATIONS (GENEVA 11864, CTB NO.79).

4. FAKELY ASKED SEVERAL QUESTIONS ON TECHNICAL DETAILS OF THE AUTHENTICATION SYSTEM. WHAT WAS THE CAPACITY OF THE READ ONLY MEMORY WHICH STORED THE KEYWORDS? TURNBULL REPLIED THAT IT HAD NOT BEEN FINALIZED, BUT WOULD BE LARGE ENOUGH SO THAT REPLACEMENT WOULD BE NECESSARY ONLY INFREQUENTLY. WHAT DATA RATE WAS NECESSARY TO CHARACTERIZE THE SEISMIC SIGNAL? TURNBULL USED THE SEISMIC RESEARCH OBSERVATORY DESIGN AS AN EXAMPLE, EXPLAINING THAT IT RECORDED DATA AT ABOUT 20 WORDS (OR 320 BITS FOR A 16 BIT WORD) PER SECOND. FAKLEY SAID IT APPEARED SOME DATA COMPRESSION WOULD BE NECESSARY IN ORDER TO ADD THE AUTHENTICATION WORD AND HOUSEKEEPING INFORMATION TO THE DATA STREAM, AND TURNBULL AGREED. FINALLY, FAKELY ASKED WHAT SORT OF TAMPER DETECTING SYSTEM THE US HAD IN MIND, AND WAS TOLD THAT FIBER OPTIC SEALS (SUCH AS HAD BEEN DEVELOPED FOR THE IAEA REACTOR SAFETY PROGRAM) WERE BEING CONSIDERED.

5. OSIN ASKED A SERIES OF MORE GENERAL QUESTIONS. HE ASKED WHETHER THE US INTENDED TO AUTHENTICATE THE DATA FROM INTERNAL STATIONS IN THE SOVIET UNION AND US OR FROM ALL THOSE PARTICIPATING IN THE GLOBAL SEISMIC NET-
SECRET

SECRET

PAGE 03 GENEVA 12065 01 OF 02 132122Z

WORK, AND WAS TOLD INTERNAL STATIONS. HOW COULD THE AUTHENTICATION PACKAGE AND TAMPER DETECTING SEALS BE INSTALLED? TURNBULL REPLIED THAT HE THOUGHT THE PROCEDURES COULD BE SIMILAR TO THOSE IN THE PNE TREATY, BUT THAT THIS WOULD HAVE TO BE DISCUSSED FURTHER. HOW WOULD THE MECHANICAL FUNCTIONING OF THE SEISMIC SENSOR ITSELF BE CHECKED? TURNBULL REPLIED THAT CALIBRATION SIGNALS COULD BE SENT TO THE INSTRUMENT TO CONFIRM ITS PROPER OPERATION. OSIN THEN ASKED WHETHER THE EQUIPMENT DESCRIBED WAS ONLY AN IDEA OR HAD BEEN PUT INTO OPERATION, AND WAS TOLD THAT THE TECHNOLOGY WAS WELL ESTABLISHED AND COULD BE PRODUCED WITHOUT FURTHER RESEARCH. FINALLY, OSIN ASKED HOW THE DATA FROM INTERNAL STATIONS WOULD BE PROVIDED TO ALL TREATY PARTIES IN THE ABSENCE OF A GLOBAL SEISMIC NETWORK, AND WHETHER WE ENVISAGED USE OF THE COMMUNICATION CHANNELS OF THE WORLD METEOROLOGICAL ORGANIZATION (WMO) TO TRANSMIT THE DATA FROM THE STATIONS TO THE TWO PARTIES. TURNBULL REPLIED THAT WE FELT THE WMO CHANNELS WERE NOT ADEQUATE FOR THAT AND THAT SATELLITE COMMUNICATIONS LINKS WOULD BE REQUIRED. THIS WOULD BE DISCUSSED IN MORE DETAIL AT THE NEXT MEETING OF THE TECHNICAL GROUP.

6. OSIN THEN ASKED FOR QUESTIONS FROM OTHER MEMBERS OF

SECRET

NNN

SECRET

PAGE 01 GENEVA 12065 02 OF 02 141054Z
ACTION SS-25

INFO OCT-01 ISO-00 SSO-00 NSCE-00 DODE-00 CIAE-00

INRE-00 ERDE-00 /026 W

-----037563 141104Z /10

O 132040Z DEC 77

FM USMISSION GENEVA

TO SECSTATE WASHDC IMMEDIATE 4024

INFO AMEMBASSY LONDON PRIORITY

AMEMBASSY MOSCOW PRIORITY

S E C R E T SECTION 02 OF 02 GENEVA 12065

C O R R E C T E D C O P Y (TEXT)

EXDIS/USCTB

THE SOVIET GROUP. BOCHAROV ASKED WHETHER THE SEISMOMETER WOULD BE AN INTEGRAL PART OF THE STATION PACKAGE OR IF IT WOULD BE PROVIDED BY THE HOST, AND WAS TOLD IT WOULD BE PART OF THE ENTIRE PACKAGE. NOVIKOV ASKED WHETHER, IF A THREE COMPONENT SEISMOMETER WAS USED, ALL CHANNELS WOULD BE AUTHENTICATED. TURNBULL SAID THAT SINCE THE DATA WOULD BE MULTIPLEXED INTO A SINGLE CHANNEL, IN THAT SENSE ALL CHANNELS WOULD BE AUTHENTICATED. NOVIKOV ASKED A SECOND QUESTION ABOUT WHETHER PROVISION WOULD BE MADE FOR VERIFYING THE RELIABLE OPERATION OF THE AUTHENTICATION SYSTEM ITSELF. HE NOTED THAT IF THIS SYSTEM FAILED, THERE COULD BE GROUNDLESS POLITICAL REPERCUSSIONS. TURNBULL NOTED THAT CHECKS COULD BE BUILT INTO THE AUTHENTICATION SYSTEM, INCLUDING REDUNDANT CIRCUITS AND A PROVISION FOR "VOTING" TO CORRECT ERRORS.

7. OSIN REMARKED THAT HE FELT CLOSER TO AN UNDERSTANDING OF THE AUTHENTICATION SYSTEM, BUT FELT THAT OTHER AUTHENTICATION METHODS MIGHT BE USED WHICH HE WOULD BE PREPARED TO DISCUSS AT THE PROPER TIME.

SECRET

SECRET

PAGE 02 GENEVA 12065 02 OF 02 141054Z

8. FAKLEY CLOSED THE MEETING, SAYING THAT THE NEXT
MEETING OF THE GROUP WOULD BE SET BY HEADS OF DELEGATIONS
BUT THAT HE FELT ANOTHER MEETING LATER THIS WEEK WOULD
BE BENEFICIAL. WARNKE

SECRET

NNN

Message Attributes

Automatic Decaptioning: Z
Capture Date: 01-Jan-1994 12:00:00 am
Channel Indicators: n/a
Current Classification: UNCLASSIFIED
Concepts: NEGOTIATIONS
Control Number: n/a
Copy: SINGLE
Sent Date: 13-Dec-1977 12:00:00 am
Decaption Date: 22 May 2009
Decaption Note: 25 YEAR REVIEW
Disposition Action: RELEASED
Disposition Approved on Date:
Disposition Case Number: n/a
Disposition Comment: 25 YEAR REVIEW
Disposition Date: 22 May 2009
Disposition Event:
Disposition History: n/a
Disposition Reason:
Disposition Remarks:
Document Number: 1977GENEVA12065
Document Source: CORE
Document Unique ID: 00
Drafter: n/a
Enclosure: n/a
Executive Order: X3
Errors: N/A
Expiration:
Film Number: D770464-0293
Format: TEL
From: GENEVA
Handling Restrictions:
Image Path:
ISecure: 1
Legacy Key: link1977/newtext/t19771263/aaaacbba.tel
Line Count: 177
Litigation Code IDs:
Litigation Codes:
Litigation History:
Locator: TEXT ON-LINE, ON MICROFILM
Message ID: b4b4c305-c288-dd11-92da-001cc4696bcc
Office: ACTION SS
Original Classification: SECRET
Original Handling Restrictions: EXDIS
Original Previous Classification: n/a
Original Previous Handling Restrictions: n/a
Page Count: 4
Previous Channel Indicators: n/a
Previous Classification: SECRET
Previous Handling Restrictions: EXDIS
Reference: n/a
Retention: 0
Review Action: RELEASED, APPROVED
Review Content Flags:
Review Date: 01-Dec-2004 12:00:00 am
Review Event:
Review Exemptions: n/a
Review Media Identifier:
Review Release Date: n/a
Review Release Event: n/a
Review Transfer Date:
Review Withdrawn Fields: n/a
SAS ID: 261483
Secure: OPEN
Status: NATIVE
Subject: CTB NEGOTIATIONS: INFORMAL TECHNICAL WORKING GROUP, DECEMBER 13, 1977 CTB MESSAGE NO.85
TAGS: PARM, US, UK, UR
To: STATE
Type: TE
vdkgvwkey: odhc://SAS/SAS.dbo.SAS_Docs/b4b4c305-c288-dd11-92da-001cc4696bcc
Review Markings:
Margaret P. Grafeld
Declassified/Released
US Department of State
EO Systematic Review
22 May 2009
Markings: Margaret P. Grafeld Declassified/Released US Department of State EO Systematic Review 22 May 2009